Revista catalana de dret públic #58

www.rcdp.cat

HOW TO BUILD E-GOVERNANCE IN A DIGITAL SOCIETY: THE CASE OF ESTONIA

Katrin Nyman Metcalf*

Abstract

The article explains and discusses the meaning, content and benefits of e-governance, using the example of Estonia. E-governance does not have to be legally complex, but it is necessary to understand and analyse the implications of new technologies. In Estonia, all public databases are linked, providing the possibility to apply the once-only principle. Individuals have easy overview of data held about them and how they are used. E-services are citizen-centric and accessed with the ID card and codes that all citizens and residents have. By explaining the Estonian example and its legal implications, inspiration may be given to other countries.

Key words: e-governance; Estonia; once-only; data protection; digital society.

COM CONSTRUIR LA GOVERNANÇA ELECTRÒNICA EN UNA SOCIETAT DIGITAL: EL CAS D'ESTÒNIA

Resum

L'article explica i aborda el significat, el contingut i els beneficis de la governança electrònica, utilitzant l'exemple d'Estònia. La governança electrònica no ha de ser complexa legalment, però cal entendre i analitzar les implicacions de les noves tecnologies. A Estònia, totes les bases de dades públiques estan connectades, proporcionant la possibilitat d'aportar dades una única vegada (once-only principle)*. Els individus tenen fàcilment una visió de conjunt de les seves dades i de com s'utilitzen. Els serveis digitals estan centrats en les persones i són accessibles mitjançant targetes d'identificació i codis a l'abast de tota la ciutadania i els residents. Explicar l'exemple estonià i les seves implicacions legals pot servir d'inspiració a altres països.*

Paraules clau: governança electrònica; Estònia; principi d'una única vegada; protecció de dades; societat digital.

* Katrin Nyman Metcalf, Adjunct Professor of Communications Law, Tallinn University of Technology and Programme Director of Research and Legal Issues, E-Governance Academy, TalTech Law School, Akadeemia tee 3, 12618 Tallinn, Estonia. katrin.nyman-metcalf@taltech.ee.

Article received: 23.04.2019. Blind review: 12.05.2019 and 19.05.2019. Final version accepted: 26.05.2019.

Recommended citation: Nyman Metcalf, Katrin. (2019). How to build e-governance in a digital society: the case of Estonia. *Revista Catalana de Dret Públic*, (58), 1-12. https://doi.org/10.2436/rcdp.i58.2019.3316

Summary

1 Introduction

1.1 E-governance: What is it and why do we need it?

An important element of the digital society is the increased use of e-governance: using digital tools for governance. This can be observed globally. Developing states as well as the richest countries in the world work on similar projects, as digital tools can be the same in different circumstances, with some adjustment to local conditions. It is interesting to note that, regarding e-governance, the richest and most stable states are often not the most successful and innovative—in fact, the opposite may even be the case. Governments that have to think about how to administer their country despite adverse circumstances often come up with exciting solutions. This is what is behind the fact that Estonia is a global frontrunner in e-governance: a country with 1.4 million people, at the edge of Europe, reindependent for less than thirty years after a long period of occupation, is used as a model to inspire countries all over the world. Globally, we are seeing many exciting examples of e-governance in developing countries in Africa, or recently democratised or transition countries. These countries are the most likely to take decisive steps and make all-encompassing reforms, making use of the same approach used in Estonia: when you have little to lose, you can leapfrog the developments others have gone through and go straight to something new.

There is no international legal definition of e-governance and the term is used differently in different contexts.[1] The promotion of e-governance has been both fashionable and ubiquitous for decades and sometimes appears to be an end in itself, rather than a tool for improving administration (Schneiberg & Bartley, 2008: 38-39). The term "e-governance" is used interchangeably with "e-government". "Governance" is a broader concept, as "government" normally denotes the public sector organs directly linked with government functions; whereas "governance" can include a wider variety of organs and functions.[2] It is usually easier to recognise e-governance than to define it: there may be no one single understanding of what it is, or even what it is for, but there tends to be a feeling about what it could do and why it would be beneficial. Introducing e-governance can reduce corruption; it can make it easier for people, including minorities, inhabitants of rural areas or the disabled to perform administrative transactions and participate in political life; it can lead to efficiency gains and thus cost savings; it may help states attract investment and support innovation. However, these positive outcomes do not just happen merely because the technology exists. Neither is it as the techno-sceptics tend to presume, that technology will inevitably lead to things like increased surveillance, data protection infringements, alienation and discrimination. In reality, e-governance—the use of digital technologies for governance—is just a way of doing things, using new tools for performing certain acts. It is not good or bad per se: that depends on how it is used.

In Estonia, all communication with authorities can be conducted electronically, and official documents, whether public or private, can be signed digitally (Madise & Vinkel, 2014: 61). Data is electronic by default, just as, for example, the electronic version of legislation is the valid, official one. Government went paperless in the year 2000. This article discusses Estonian e-governance, describing the key elements and features that may be interesting as a model for others. It attempts to explain what is done and why, especially from the legal perspective.

1.2 Why Estonia?

When working in different countries or with delegations visiting Estonia to learn about e-governance, the question almost always comes up: How is it that Estonia is so advanced; how was it possible to do something so innovative, in the 1990s when the country had only just emerged from a long period of occupation, with an economy and an administration that were both at rock bottom? There is no single, generally-accepted answer to this question, but as the architects of the Estonian e-governance system tend to say, Estonia did it not because

1 The Council of Europe, in Recommendation Rec(2004)15, refers to Electronic Governance or e-governance without a definition, but with an understanding that the term is self-explanatory. The World Bank links the benefits of e-governance to the definition: "'E-Government' refers to the use by government agencies of information technologies […] that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions".

2 This article will use the term "e-governance".

it *had* resources but because it *had not*. There was no realistic way in which Estonia, in a reasonable length of time, could build the kind of public administration that its Scandinavian neighbours had, so the choice was between doing something quite different or remaining behind for decades. Fortunately, Estonia had politicians and administrative officials who made the most of the fact that there really was nothing to lose. A culture of risk-taking and a highly educated population helped, but the process soon became self-perpetuating, as the interest and enthusiasm that many early ideas were met with gave the impetus to try more new things. Estonia is one of the countries in the world with the most start-ups per capita, as interest in innovation—especially with new technologies—creates its own momentum. Many e-governance solutions were born out of public private partnerships or lead to cross-fertilisation between the public and private sectors.

It is a little easier to answer the question of what it is that sets the current Estonian system of e-governance apart from that of other states. Estonia is no longer alone in using e-governance tools. It does not even top the various rankings on the issue. To some extent, this is due to the nature of the rankings, whose measurement criteria may become outdated, given the rapid development of technologies, putting the most innovative states at a disadvantage. There may also be solutions in other countries that are at least as useful and exciting as those in Estonia, but global interest in Estonia as a model does not appear to wane. One of the reasons for this may be that a country that undertakes reforms, despite not being rich or having a long history of stable development, may be a model that is easier for others to emulate. However, it is also true that the Estonian e-governance system is used by wide segments of society, for a variety of different services. In many countries, popular uptake of e-services tends to be uneven or slow, which easily leads to a vicious circle: those developing services feel it is not justified to put a lot of resources into something only a few people use, while people are disinclined to learn how to use the services, or obtain the devices needed to do so, if there is not a great deal they can do with them.

2 Components of e-governance

2.1 The building blocks of e-governance

The exact nature of e-governance in a specific country or situation has to be described in that specific context, as it is part of *governance*—something that is different in different countries—with the electronic side of it being just a way of doing things. Not all use of digital tools necessarily leads to sufficient changes in governance for us to be able to legitimately talk about a transition to e-governance. From a legal perspective, it is important to know the specifics of what one is talking about, as different kinds of electronic tools can have different legal implications. Countries talk about introducing e-governance when they facilitate access to information by electronic means, without any interactivity: basically, just having websites of ministries and authorities. We presume for the purposes of this article that "real" e-governance has to contain elements of interactivity and interoperability. This means that it is possible to perform some transactions online and that databases can communicate with one another so that there is not only a set of isolated electronic services, but some form of totality (Nyman Metcalf, 2017).

Both interactivity and interoperability entail consequences for the legal system. These consequences do not necessarily mean new and special legislation. Indeed, one of the key rules for a successful legal approach to e-governance is *not* to adopt too much special legislation, as this risks creating parallel systems that focus on the way things are done rather than the substance of what is done. Rule of law, as well as the protection of fundamental rights, are values that can and should remain in an era of automation, without the need for far-reaching changes in legislation. For this to be possible, it is nevertheless important to understand what, how and why that change is processed, and how it is perceived by people. With this knowledge, what needs reflection in the legal system can be distilled to better protect rights and strengthen the rule of law. This was the approach chosen in Estonia, which means that the country does not have a great deal of legislation specific to e-governance.

2.2 Interactivity

Interactivity is a key concept in explaining the difference between using digital tools for sharing information and using them to perform administrative tasks. Accessing information online is very important and can be a crucial step towards a more transparent administration. From the legal side, it is uncomplicated: provided that the information is public, there is no need to identify oneself and the public body that posts the information does not need to know who looks at what or why. Indeed, in some countries it is explicitly prohibited to ask why people want to access public information, so as not to have a chilling effect on such demands. Regardless of the importance of access to information, the real difference to the administration comes when it becomes possible to perform transactions online. At this point, some form of electronic identification also becomes necessary (Wang, 2006).

Identifying oneself electronically needs to be secure, but at the same time user-friendly. Specific identification systems can be used for different services, but such a system is rarely user-friendly. Thus, an identification system that is secure and legally recognised for all kinds of transactions is preferable. That said, it is important to stress that, just because Estonia has such a system and this is no doubt part of the reason for the success of Estonian e-governance, it is not a requirement to do exactly as Estonia has done. It is, however, a requirement to have some form of electronic identification. The Estonian system is a good example of public-private partnership, as initially e-services were mainly accessed with bank ID, while now most people perform banking transactions with the official ID. The state and the private banks agreed to accept each other's identification systems, which they mutually deemed sufficient for the transactions.

A digital signature, as the name implies, means that the information is broken down into digital format and can be read with the correct codes to retransform the digital into legible format. A digital signature requires codes of some sort; a device may be needed to create or transmit the codes. From a legal viewpoint, the digital signature looks different to a traditional one, which means that there must be provisions in law to explain what it is and how it is created. Several digital signature concepts are in need of clarification, which may be self-evident for traditional signatures.

When deciding what kind of signature or other identification should be required, it is essential to determine whether the identity is capable of fulfilling the function of authenticating a person. It is important to consider the risks of intervention, modification or technical compromise. Although there are many possible forms of digital identification, it is common for secure electronic signatures to consist of different keys, a private and a public one. These are linked to the certification authorities that issue and control the identification systems that ensure the validity of the signature (Wang, 2016).[3] The law needs to ensure acceptance of e-signatures (Malkawi, 2007: 163), which must have the same force as regular signatures and such force shall be provided by law.

Estonian public administration is based on citizen-centric electronic services in all areas, accessed from one web portal, www.eesti.ee, and in the same manner for all services, which makes them easy to use. The access is made with the digital identity that all citizens and residents have (https://e-estonia.com/solutions/e-identity/id-card). Legislation on population registers sets out the principles for the unique personal identification code—a unique, lifelong, 11-digit code mandatory for everyone in Estonia—that is the key to services. The ID code is given to children at birth and to immigrants when they move to Estonia. Adults are obliged to have an ID card, to which codes for electronic use are attached: a four-digit number to enter the system and a five-digit number for the digital signature. It is not compulsory to use electronic services, but the possibility of using them is automatically attached to all ID cards and not something that has to be requested separately. A special card reader is used for computers, which may be built into computers sold in Estonia or otherwise attached via a USB port. The small device costs around 10 euros, and there are different versions, but it is often given free of charge, by banks, for example. It is also possible to use a mobile ID, for which no special device is needed; it is linked to the SIM card and is requested from the telephone operator. As opposed to use of the ID card, which is free, use of the mobile ID entails a charge, to the operator, of normally about one euro per month. The most recent identification possibility is a so-called Smart-ID, also linked to the mobile telephone, but this is not yet usable for all transactions.

3 This aspect has been recognised by courts as a reason for not accepting electronic means of signing. Wang refers to German court cases.

The ID card is also usable as identification "in real life" and, for Estonian citizens, as a travel document within the European Union and a few additional countries. It is thus a document that everyone has and normally carries with them, which means no additional effort is needed to use the digital ID. In addition to electronic transactions, the same personal code applies in all other contexts where personal identification is necessary. The fact that the same card and code serves many purposes helps make services accessible. It is sometimes claimed that all the data needed for any e-services is on the chip in the ID card, but this statement is not correct, as the ID card and the identification codes linked to it merely act as a key that opens doors to various databases; nothing is stored on the card itself.

2.3 Interoperability

An important enabler for seamless and efficient public services is the interoperability of databases. The Estonian system is called X-road. This is an interface that allows different databases to communicate. Databases can communicate directly with each other, which means that authorities in need of data that exist in any public database can access this database directly rather than create their own. This allows the practical application of the once-only principle, which means that a person never has to provide data more than once to the authorities, strengthening the integrity of the data. If the data already exists in a database, it has to be used from that database. It is prohibited by law to create a database with information that already exists, and persons should not be asked to provide the same information more than once (Public Information Act, English translation, see https://www.riigiteataja.ee/en/eli/514112013001/consolide). This system is secure, as it eliminates the need for officials to have to request data and the need to send data between authorities. Such situations of requesting and sending data are points of risk for data protection as well as for data accuracy. In Estonia, if it is determined that someone needs access to data, that person is provided with the opportunity to go directly to the source and access the data via the X-road.

Interoperability of databases thus makes it possible to use data from the original source database, avoiding duplication but also avoiding large, centralised databases. The Administrative Procedure Act (English translation, see https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012018001/consolide) contains requirements of efficiency, which is supported by the X-road. Here it is essential to point out that actual data use is regulated by service level agreements between authorities on data sharing. Just joining the X-road does not give the organs in the system automatic access to the data of others; agreements are needed to specify exactly what type of data individuals in different organisations shall have access to. For each data access, the person who wants to look at the data must identify him- or herself, as the access is given to the person and permitted via their digital identity. There is no such thing as a "ministry computer" or "authority computer", on which anyone who can access the device can see personal data that belongs in the area of the authority in question. To see any data, everyone first has to show the system who they are, with their ID card and digital identity, as access to data via the X-road is given to individuals, not organisations.

Estonia had a law on databases from 1997 until 2002, when the law was repealed. Since then, the key provisions on databases (how to create or close them, basic requirements for data, etc.) are instead found in the Public Information Act. Interoperability requires a basic level of unified standards of data as well as cooperation between organs, but each body holding a database can still decide most issues about it itself. Key legal provisions are found in the X-road regulation, the Data Exchange Layer of Information Systems (RT I 2008, 18, 129, entry into force 8 May 2008), and in the Government Regulation on System of Security Measures for Information Systems (Regulation 252, 2007, RT1. I, 71, 440, entry into force 1 January 2008, based on Article 439 (1) 4) of the Public Information Act). Having detailed rules on what is needed to enable interoperability in sub-legal acts is a conscious choice, as these rules must be flexible and able to change, if and when new technology raises new questions. There is no need for all databases to look identical, but legislation and regulation provide rules on what is needed to make interoperability—communication between the databases—possible.

3 The law of e-governance

3.1 Legal prerequisites for e-governance

Legal issues of e-governance do not form a single, unified area of law. E-governance is perceived as something new and highly technological, a complex collection of technical requirements for how to prove identity, how to protect infrastructure, how to share data and interact with different parties. It is quite common that, when states begin to prepare for e-governance, they do not involve lawyers until a later stage of the reforms, as the matter is seen as an IT issue. Secondly, once the lawyers do get involved, they are often tempted to start drafting specific rules that match the complexity and comprehensiveness of the technology. This is not, however, the most efficient and secure way to deal with the legal aspects of e-governance. What is needed is not complicated technical legislation, but an overview of legislation to ensure that e-services are integrated and attention has been paid to digital identities and signatures as well as to data protection. To be able to enjoy the benefits of e-governance, it is important to see it as an integral part of the legal and administrative system of the country, with e-services well integrated into whatever legislation or systems are available for service delivery. The previous Estonian President, Mr Toomas Hendrik Ilves, used to say that Estonia does not have a digital society: Estonia *is* a digital society. The key principle to be followed in order to create a coherent legal framework for e-governance is simple: there should not be too many special laws, as only by integrating e-governance with regular governance at all levels can it be a part of the state system and help obtain efficiency and other gains already mentioned.

In addition, too much regulation of technical matters may stifle innovation. Over-regulation can lock in technologies when what is needed instead is flexibility, as technology moves so fast. Laws and other forms of regulations should address the nature of services and transactions or the type and sensitivity of data, in a technology-neutral manner. Instead of concentrating on the technologies used, the background to what kind of regulation to adopt should be the issues dealt with, and the aspects of governance that are to be handled electronically, rather than (just) in the traditional, paper-based manner. This apparently self-evident suggestion is surprisingly often not implemented in practice. In Estonia, the legal system from the start was designed to see e-governance as an aspect of governance, with as few special rules as possible. Many people expect to find a large number of special e-governance laws in Estonia, but this is not the case. Not creating special "e" legislation helps to ensure that the benefits of e-governance can permeate the legal and administrative system of the country and that e-services are integrated into general laws governing the various services.[4] The legal environment consists of specific and technical rules, based on a legal mandate given to stipulate sufficient criteria for a system of interoperability to function.

A key factor determining successful transition to e-governance is the establishment of a governing authority responsible for different aspects of e-governance. The competence of this agency must be set out in law to avoid ambiguity and disputes. Such a well-functioning body, capable of adopting the relevant rules as well as ensuring their implementation, may be what determines the success of e-governance.

3.2 The importance of trust – and the role of law in trust

For people to embrace e-governance, they need to have trust in the services provided in this new manner. This includes being able to identify oneself electronically in a way that is easy to use and secure—as well as being perceived to be secure. It includes the need to feel that what happens with data is transparent and secure. The EU General Data Protection Regulation 2016/679 (GDPR) is an important tool for increasing trust. Trust also requires the knowledge that transactions performed electronically will be just as valid as traditional transactions, even if needed as evidence in court. Although trust is not merely a legal matter and cannot be created by legislation alone, law is a key component of trust-building. Legislative questions of e-governance may include general, even mundane, questions of administrative or procedural law and how to adapt these to the new technologies used. What is important is an analysis of the legal system to identify potential obstacles for the use of e-services, such as form requirements (decisions have to be handed down

4 "Noting that e-governance is about democratic governance and not about purely technical issues, and convinced therefore that the full potential of e-governance will be harnessed only if ICTs are introduced alongside changes in the structures, processes and ways that the work of public authorities is organised", Preamble, Council of Europe Recommendation Rec(2004)15 adopted by the Committee of Ministers of the Council of Europe on 15 December 2004 and explanatory memorandum, www.coe.int.

on blue paper, something requires underlining in red ink, a person needs to raise their right hand, and so on—any language that does not fit in the electronic world), and ensure the necessary adjustments are made. Functioning e-governance will help to build trust, while problems of even a basic practical nature can soon erode trust.

The protection of human rights may be strengthened by the use of electronic tools, but such aspects will not be appreciated by the population at large if they are not presented and promoted. In many countries, a majority of people still feel that electronic data is more vulnerable than paper-based data (Nyman Metcalf, 2014a). To some extent, this may be a generational issue, but there are also other reasons. The new operations that can be performed thanks to electronic data and automatic data processing, such as face recognition or, generally, the compilation of enormous amounts of data that at least in practice would be impossible to do manually, do entail new risks. It is no coincidence that an instrument such as the GDPR has been adopted now. In addition, as people provide so much data to social networks, commercial firms and to each other, there are understandably instances of personal information being abused, or at least too widely known. When appreciating the risks, most people do not make a distinction between such issues and the public sector use of data, where—in democratic rule-of-law states—there are stronger protection systems in place and fewer problems. No one likes to hear that the main problems are self-created: you cannot expect privacy if you put your life on social media like Instagram or Facebook. However, it cannot be ignored that this leads to people having an uneasy feeling about electronic data that may lead to scepticism regarding e-governance. We cannot say that they should just know better and understand the distinctions. An arrogant approach to people's fears and hesitations is not only wrong in a democratic society, it will also be counterproductive for the development of e-governance. If people do not trust services, they will not use them. A state cannot justify spending money on transitioning to a new form of governance if it is merely a niche project, used by an elite, while the traditional ways of storing data and providing services go on in just the same way as before. In such a case, the efficiency gains of e-governance will not be felt, nor can improved protection of rights be fully explored.

Trust is to some extent created by symbols. The word "symbols" here should be seen in a broad sense: the impressive style of buildings, judges' robes, the elaborate letterheads on official letters, are all symbols of power, of the state. Such symbols help to create the impression people have of the state, including whether they trust it, whether they feel that they should follow rules made by the state and whether these rules are there for a legitimate reason. What the e-state will mean for our impression of the state as such is still early to say, but it is already necessary to think about how symbols can also be used in the electronic world to create the trust that is a necessary prerequisite for successful governance in a rule-of-law state.

One of the elements of Estonian e-governance that attracts the most attention globally is the fact that, in Estonia, since 2005 it has been possible to vote in all elections (local, national and European) over the internet (https://www.valimised.ee/en/internet-voting/internet-voting-estonia). This is unique in the world, although there have been some smaller trials in Norway and Switzerland and other specific situations elsewhere. These elections have been a success in Estonia, with no reported problems and more people using the internet voting option at each election: more than a third of all voters (OSCE, ODHIR, 2011: 6). The fact that Estonians are happy to allow this system to be used for something as important and sensitive as voting indicates that the level of trust in electronic services is high. The system is continually being tested and improved, from the technical as well the legal perspective. One relatively recent addition is that it is easier to trace that a vote has been counted. Although there was no reported issue with votes not reaching the stage where they are counted, people were worried about this, so a feature enabling voters to check this online was added. It is a good example of how concerns need to be addressed, even if perhaps the concern is not actually relevant from a technical perspective, not least given the important symbolic role of elections.

The best way to illustrate the voting system is to think of it as an envelope system, like many paper-based systems: the identification of a person is put, together with a sealed envelope with a vote inside, into an outer envelope. This envelope is opened and it is seen who has voted, so that no more than one vote per person can be counted. At the same time, the envelope with the vote is divided from the identification in such a manner that it is impossible to trace who submitted which vote, and only after that is the inner envelope opened and the vote counted. This process will be well-known for people who have been involved in any voting process.

The difference is that all these envelopes, and all the counting, ticking-off, etc., are electronic. If the aspects of how votes are counted did not raise problems in the electronic world, the question of voting in any location without guarantees against someone influencing how you vote was more complicated. This has been solved so that it is possible to vote again, though only the last vote will be counted. The idea is that a person will have the possibility to avoid whomever it is that tries to influence them, at some point. At its inception, the voting system was examined by the Supreme Court in 2005 (Judgment of the Constitutional Review Chamber of the Supreme Court number 3-4-1-13-05) following a complaint by the President in his capacity of examining the constitutionality of legislation. The case centred on the principle of one person-one vote and whether e-voting ensured this. The Court found that there was nothing in the system that compromised the principle of one person-one vote, as the counting only ever allows for one vote; it does not even see additional ones, as these are discarded by the system when a new vote is cast. The Supreme Court ruled that the system of e-voting appropriately balanced all electoral principles of the constitution—including what to do if you vote in an environment where others around you may try to influence you (Madise & Vinkel, 2014).

3.3 Data Protection

Special focus should be given to data protection legislation, given the paramount role of data for e-governance. Electronic data may not be less secure than traditional paper-based data—the reverse may even be true—but there is more intense data use and concerns may cause people to be wary of e-transactions. Insufficient data protection legislation may also mean that loopholes for data security are abused. In data protection, as in many other areas, law and technology should work together, with technical solutions employed to protect data and the law requiring such solutions. Estonia, like all EU member states, applies the GDPR, which sets the framework for data protection.

The use of e-governance tends to be presented as if there were a need to weigh up whether the benefits of efficiency and speed make up for data protection risks. What is less well understood is that e-governance solutions and use of electronic data can, if properly used, provide greater data protection than traditional, paper-based data, thanks to the possibility of traceability. In Estonia, one of the important features of the interoperable data system, the X-road, is that individuals (citizens or residents of Estonia) can easily see what data the authorities hold on them, by accessing one web-site (https://www.eesti.ee) from which all public services and databases can be reached (Nyman Metcalf, 2014b). Whenever an authority accesses the data of an individual, this leaves a footprint, which the person can easily see. It says which authority looked at the data and at what time, and the person is entitled to ask the authority to explain why they did so. Within the authority, it is also possible to see which person accessed the data, as all data access is only possible after the authorised person has identified themselves, with the usual ID card and codes. As mentioned above, authorisations for access to data are not given per authority, but specifically, determining which persons can access what type of data. As the person must identify him- or herself for each data access, there is no risk of careless access to data or abuse of access rights out of curiosity because there is a real risk they will be called on to explain the purpose and proportionality of the data use (Rull, Täks, & Norta, 2014). Not only can individuals see who accesses their data, but controls are conducted both within authorities and by the data protection inspectorate, who will react if unusual or unexplained data access appears to have occurred (Nyman Metcalf, 2017).

Data protection is a human right, derived from the right to privacy. In Europe, the right is protected by the European Convention on Human Rights through its provisions on protection of privacy, Article 8, as well as by the Charter of Fundamental Rights of the European Union, which is the first international instrument to have an explicit data protection provision that includes the right to access and rectify data about oneself and the need for control by an independent authority (Article 8), in addition to the general privacy protection (Article 7). By mentioning data protection specifically, the Charter of Fundamental Rights underlines its importance, not least against an increased use of ICT (Nyman Metcalf, 2014a: 28-30). The essential issue is the content of the data, and whether it is of a sensitive nature. Although ICT has meant there are many more ways in which data can be used—and also that combinations of data or IT data processing can generate potentially sensitive knowledge that might not have been generated by manual manipulation of the same data—in most cases the sensitivity of data is actually much less dependent on its form (electronic or not) than on its content. Legislation needs to focus on the risks and identify what measures are needed to deal with

these risks, rather than trying to make rules for everything just because it is new and different (Brownsword & Goodwin, 2012).

Several of the tools used in Estonia for data processing mean that it was easier for Estonia to meet the requirements of the GDPR than for some other countries. The very individualised data access possibility, coupled with the fact that anyone with access to personal data may find themselves obliged to explain the purpose of the data use, is one such aspect. For the private sector, where data use is generally based on consent, in Estonia as elsewhere, the GDPR meant new or different requirements for companies to ensure that consent is properly given and data properly processed.

In terms of perception of and trust in e-governance, data protection is important. Governance and the public services offered through e-governance are largely not voluntary, and if a state expects its subjects to provide data within the framework of various public services, it must also ensure that people have faith in the system. It is different to commercial services, where individuals can choose whether to use them or not. It is not as if data protection is not important also for such services, but as there is always the option of not using something, we can expect people to make more conscious choices, depending on how comfortable they feel with a certain service. In the case of e-governance, the state is under obligation to provide this feeling of comfort. Successful e-governance is built around interoperability of databases, meaning that data held in various databases can be used seamlessly by different authorities and for different contexts. This could mean, however, that any breaches of data protection could have widespread negative consequences.

4 The future

4.1 Invisible government

Estonia started early and placed itself ahead of many countries as far as e-governance is concerned. We will not stay ahead if new developments are not made, however. Automation and the use of artificial intelligence permits proactive government whereby, not only is it easy to submit digital applications, but now you do not need to apply at all: decisions are made automatically, based on data that exists in databases. This is a new concept of government and governance, where individuals do not need to apply for things—or even contact the authorities at all—unless they want to do something other than what is expected and mostly done in a certain situation. The government process is set in motion at the birth of a child which is registered, and the child is given an identifier. From that moment, child benefit is determined, the child is assigned a doctor, it is registered for a future place in a kindergarten and school, and so on. If the parents do not want a place in a kindergarten for example, as they arrange alternative child care, they can inform the appropriate authority in a simple, electronic manner; but if they have no special requests, decisions will be taken without the need for them to apply for anything. Special needs due to medical conditions and similar will be known by the system, as they are entered into the relevant databases by authorised professionals (medical personnel), so these are also taken into account when decisions are taken. Most of the data required already exists in governmental systems, so the new aspect is not one of collecting more data but rather how this data is handled.

In Estonia, there is some legal potential to presume the will of persons, and some services are already pro-active. A Government Regulation from 2017 on Principles for Managing Services and Governing Information (adopted 3 June 2017, entry into force 7 July 2017)[5] stipulates in Article 2 that "proactive services are the direct public services provided by an authority on its own initiative in accordance with the presumed will of persons and based on the data in the databases belonging to the state information system. Proactive services are provided automatically or with the consent of a person". The way proactive services will be provided are generally as services based on life events, rather than on applications, and the Regulation introduces the notion of event services. These are the direct public services, provided jointly by several authorities, so that a person is able to perform all the obligations and exercise all the rights arising out of an event or situation. Even if several services are related to the same event, these will be fused into a single service for the user. The existence of interoperable databases and unique identifiers permit such proactive services.

5 English translation available at https://www.riigiteataja.ee/en/eli/507072017004/consolide, adopted under subsection 27(3) of the Government of the Republic Act and subsection 6(2) of the Archives Act.

The number of proactive, life-event services is expected to increase in the near future. Special legislation already sets out rules for certain proactive, specific services. For example, pensioners who live alone receive special monetary support, which is based on the data that can be seen from registries: that a person is a pensioner and that they live at an address where no one else is registered as living. In such case, the support is paid out automatically. The person has the right to challenge the decision, but as such decisions are used in cases where the action is beneficial to the person, it is rare for there to be challenges. On the other hand, a person who does not automatically get the support but feels they are entitled can apply for it and the application will be looked into.

4.2 Is it a new society?

Society has changed more rapidly in the last decades than in previous centuries. Even if it is tempting for any era to consider its changes as more important than those that have gone before, there is evidence that new technologies are spreading more rapidly in recent times and affecting more elements of our daily lives. Internet permits communication and interactivity which is almost instantaneous, just as in ancient tribal societies (Dutt & Kerikmäe, 2014: 41). Our increasing ability to perform various kinds of transactions without direct human contact, via different electronic means, is a change that not only affects social relationships but also governance (Hood & Margetts, 2007: 202). From this viewpoint, it also affects the protection of fundamental rights and may influence the rule-of-law nature of society. Saying that it affects these matters precludes any judgement about whether it weakens or strengthens the protection of rights, but it does underline the need to think about what is affected and how; and, if there is an effect, how to ensure that new ways of doing things will not weaken the protection of rights or the right to fair, efficient and rule-based governance.

The legal and social side of e-governance tends to be less well-studied than the technical one. This is despite the fact that, in many ways, the "soft" side of e-governance development may hold the key to it being able to meet the ambitious targets set for it. The recognition of what e-governance means is in many ways still in its infancy in many countries. At any internal or inter-ministerial working group, international forum or e-governance conference, one tends to meet predominantly IT technical people. This is the case even if the subject for the event is the legal and regulatory framework of e-governance. It is not unusual that IT departments are made responsible for questions of access to information or data protection. Even if the ICTs used are no longer very new, there is still a prevalence of the idea that technology should guide the regulation and that those who understand technology are thus best placed to deal with the regulatory issues as well.

However, instead of focusing on the complexities and the differences, those involved—including those involved with drafting legislation—should first of all take a step back and see what actually is different, and not just that the environment in which it happens is different. The use of e-governance should mean that governance really is for the citizens and not the other way around. Citizens, residents and companies no longer need to go to a place at a time chosen by the authorities, but the authorities come to the people, when and where it suits individuals. Technological tools and digital data can make this worthy aim possible in practice. And if this happens, e-governance becomes a tool for increased trust and participation, leading to a citizen-focused society which supports the rule of law. This does not have to remain just a beautiful policy pronouncement, met with scepticism as are most such pronouncements, eventually buried under regular bureaucracy. ICT can be truly transformative.

Reference list

Brownsword, Roger & Goodwin, Morag. (2012). *Law and the technologies of the twenty-first century*. Cambridge: Cambridge University Press.

Dutt, Pawan & Kerikmäe, Tanel. (2014). Concepts and problems associated with eDemocracy. In: Tanel Kerikmäe (Ed.), *Regulating eTechnologies in the European Union* (pp. 285-324). Heidelberg: Springer.

Hood, Christopher C. & Margetts, Helen Z. (2007). *The tools of government in the digital age*. Basingstoke: Palgrave Macmillan.

Judgment of the Constitutional Review Chamber of the Supreme Court number 3-4-1-13-05 [Petition of the President of the Republic to declare the Local Government Council Election Act Amendment Act, passed by the Riigikogu on 28 June 2005, unconstitutional, 1 September 2005]. Retrieved from http://www.nc.ee/?id=823

Madise, Ülle & Vinkel, Priit. (2014). Internet voting in Estonia: From constitutional debate to evaluation of experience over six elections. In: Tanel Kerikmäe (Ed.), *Regulating eTechnologies in the European Union* (pp. 53-72). Heidelberg: Springer.

Malkawi, Bashar H. (2007). E-commerce in light of international trade agreements: The WTO and the United States-Jordan trade agreement. *The International Journal of Law and Information Technology, 15*(2), 153-169.

Nyman Metcalf, Katrin. (2014a). The future of universality of rights. In: Tanel Kerikmäe (Ed.), *Protecting human rights in the EU* (pp. 21-35). Heidelberg: Springer.

Nyman Metcalf, Katrin. (2014b). E-governance in law and by law. In: Tanel Kerikmäe (Ed.), *Regulating eTechnologies in the European Union* (pp. 33-53). Heidelberg: Springer.

Nyman Metcalf, Katrin. (2017). Drafting e-governance: A new reality for legislative drafting. *International Journal of Legislative Drafting and Law Reform*, *5*(1).

OSCE, ODHIR. (2011). Estonia. Parliamentary Elections. 6 March 2011 [OSCE/ODHIR needs assessment mission report].

Rull, Addi; Täks, Ermo & Norta, Alexander. (2014). Towards software-agent enhanced privacy protection. In: Tanel Kerikmäe (Ed.), *Regulating eTechnologies in the European Union* (pp. 73-94). Heidelberg: Springer.

Schneiberg, Marc & Bartley, Tim. (2008). Organizations, regulation, and economic behavior: Regulatory dynamics and forms from the nineteenth to twenty-first century. *Annual Review of Law and Social Science*, *4*, 31–61.

Wang, Minyan. (2006). The impact of information technology development on the legal concept: A particular examination on the legal concept of 'signatures'. *International Journal of Law and Information Technology, 15*(3), 253-274.